UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,146	06/20/2001	John E. Brezak	14917.0461US01	5712

27488 7590 10/05/2007

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
BARQADLE, YASIN M	

ART UNIT	PAPER NUMBER
2153	

MAIL DATE	DELIVERY MODE
10/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/886,146	BREZAK ET AL.	
	Examiner	Art Unit	
	Yasin M. Barqadle	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/29/2007*.

2a)☒. This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-17,19-27,29-35,38-41,43-50,52-58,60 and 61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-17,19-27,29-35,38-41,43-50,52-58,60 and 61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/05/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

2. The amendment filed on July 05, 2007 has been fully considered but are not persuasive.

- Claims 1-2,4-17,19-27,29-35,38-41,43-50,52-58 and 60-61 are presented for examination.

Response to Amendment

Applicant in essence agues "Fox does not teach or suggest delegation. According to Fox, any credential the client needs, either for the client's own use or for a proxy to use on the client's behalf, is both requested by the client and delivered to the client. The requests may pass through a proxy, but the client never delegates to its proxy authority to request for credentials itself. In fact, the only credential given to the proxy that allows the proxy to act on the client's behalf is a service ticket that the client itself requests, decrypts, and then supplies to the proxy, as described below." (Page 17 paragraph 4).

Examiner notes Fox teaches delegation. For example, Fox teaches client securely relaying it credential to Charon and the proxy interacting with service on the client's behalf. Proxy also retrieves MIME images and formats according to client's convenience without the client being involved (page 158, col. 2, second to last paragraph). Fox also teach the client placing more trust in Charon and delegating to act on its behalf, thus allowing Charon to negotiate directly on client's behalf. (Fox, Section 2.3, Page 158, Column 2, Paragraph 3). Applicant's arguments that Fox does not teach delegation are contrary to what the Applicant has admitted in prior arguments. See page 16, second paragraph "Thus, the passage of the cited reference relied upon by the Office Action expressly allows for unconstrained delegation." (See page 16 remarks 10/02/2006).

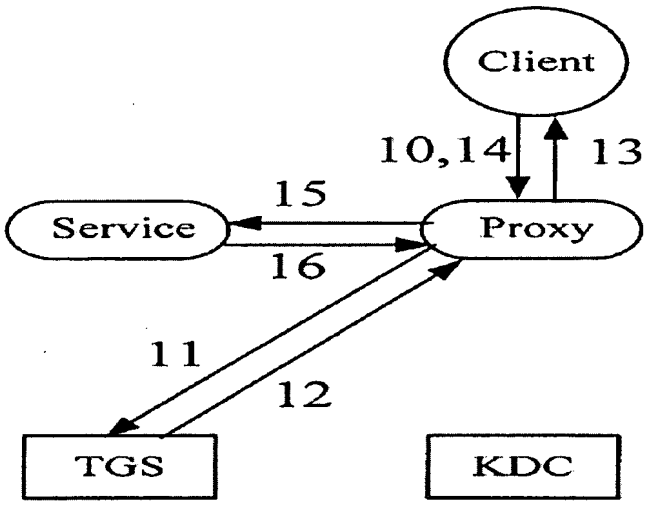
Page 161, section 4.5 steps 1 Fox teaches "Charon may be trusted with temporary session keys for particular services it contacts on the client's behalf, but not with the user's Kerberos password or with sufficient information to impersonate the user...Each time an additional

service is requested, the client cooperation is required to gain access." See also Fox, Section 2.3, Page 158, Column 2, and Paragraphs 1- 3).

Applicant argues that in Fox "The proxy is unable to obtain any service tickets without relaying messages back and forth to the client, thus, Fox does not teach delegation." Page 21, end of second paragraph. Fox also teaches "An alternative approach to service access that places more trust in Charon is for the client to reveal Kc,tgs to Charon over the established secure channel, thus allowing Charon to negotiate for Kerborized services directly. (Fox, Section 2.3, Page 158, Column 2, Paragraph 3). Furthermore, Fox teaches that Charon can construct the authenticators that must accompany the TGT on each request, and therefore does not need to interact with the client to access new services." (Fox, Section 2.3, Page 158, Column 2, Paragraph 3). This clearly shows that Fox teaches delegation where the proxy makes request and constructs the authenticators accompanying the TGT to act on client's behalf.

Examiner notes that Fox teaches, "Charon requests a TGT on the client's behalf." Page 158, first paragraph step 2. The messages may have been arranged by the client as the Applicant argues, but Charon does request a TGT and hence acts on client's behalf as required by the claim.

According to fig. 1 (d) fox shows arrows from proxy to TGS and receiving authorizing credentials and in arrow 15 shows requesting a service on clients behalf where the service results is returned in arrow 16.



(d)

Therefore, Fox teaches authorizing a server to access a target service on behalf of a client.

Additionally, the Applicant makes similar arguments regarding claim 40 and the rest of the independent claims such "Fox neither teaches nor suggests causing the server to request a service credential to itself. Again, Fox only teaches a proxy forwarding requests for service credentials. Because every request for a service credential in Fox actually is initiated by the client itself, Fox fails to suggest causing a server to request anything for itself. Fourth, Fox neither teaches nor suggests causing the server to use its own credential authenticating the server to obtain a service credential to itself. Again, every request for a service credential made by Fox comes from the client, and all such requests involve the client's own authentication credential. Fifth, Fox fails to teach constraining delegation by only "causing the server to issue the new service credential when one of: the service credential to itself indicates it is delegable; and the second authentication method trusted third-party maintains an indication that the service credential to itself is delegable. Sixth, Fox fails to teach constraining delegation by only "causing the server to issue the new service credential when one of: the service credential to itself indicates it is delegable; and the second authentication method trusted third-party maintains an indication that the service credential to itself is delegable." (Page 31 of the remarks). Examiner notes that the above responses similarly apply to these arguments. For example, see page 161 section 4.5 steps 1 "Charon may be trusted with temporary session keys for particular services it contacts on the client's behalf, but not with the user's Kerberos password or with sufficient information to impersonate the user." See also Fox, Section 2.3, Page 158, Column 2, and Paragraphs 1- 3).
Fox also teaches "An alternative approach to service access that places more trust in Charon is for the client to reveal Kc,tgs to Charon over the established secure channel, thus allowing Charon to negotiate for Kerborized services directly. (Fox, Section 2.3, Page 158, Column 2, Paragraph 3). Furthermore, Fox teaches that Charon can construct the authenticators that must accompany the TGT on each request, and therefore does not need to interact with the client to access new services." (Fox, Section 2.3, Page 158, Column 2, Paragraph 3). This clearly shows

that Fox teaches delegation where the proxy makes request and constructs the authenticators accompanying the TGT to act on client's behalf.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless —
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-46, 48-50, 52-55, 57-58, and 60-61 are rejected under 35 U.S.C. 102(b) as being anticipated by Fox et al. *("Security on the Move: Indirect Authentication Using Kerberos",* 1996, hereinafter "Fox"). Fox discloses indirect authentication using Kerberos. Fox shows,

In referring to claims 1, 4-5, 12, 16, 19-20, 26, 29-31, 33, 35 and 38

- identifying a target service to which access is sought on behalf of a client; and causing a server operatively coupled to the client to request a new service to access the target service on behalf of the client, from a trusted third party without providing a client's authentication credential: "Charon interaction consists of two distinct phases: the handshake phase, in which the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase, in which the proxy accesses Kerberized services on the client's behalf. The Charon protocol module on the proxy and the Charon client side software are responsible for the flow of control during both phases." (Fox, page 157, paragraphs 2 and 3), wherein the server provides the trusted third party with credentials authenticating the server, information about the target service, and a service credential previously provided by the client to the server allowing the client to access the server *"During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy. From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase. "* (Fox, page 157, paragraph 3); and

  causing the trusted third party to provide the server with the new service

credential that authorized the server to access the target service on behalf of the client (see section 2.3 where Charon does not have user's Kerberos password), (the Charon client-side never reveals the user's Kerberos key to anyone.. Charon module cannot obtain service on behalf of the client without the client's explicit cooperation (page 157 end of section 2.1 and section 2.2 number 6-7. Note forwarded message contains the (encrypted) TGT. See 4.5 steps 1-3 Charon may be trusted with temporary session keys for particular services it contacts on the client's behalf, but not with the user's Kerberos password or with sufficient information to impersonate the user...See also Fox, Section 2.3, Page 158, Column 2, Paragraphs 1- 3); and

when one of::

the service credential specifies that delegation of the service credential is authorized (Fox, Section 2.3, Page 158, Column 2, Paragraphs 1- 3); and the trusted third-party maintains an indication that the delegation of the service credential is authorized. (Fox, Section 2.3, Page 158, Column 2, Paragraphs 1- 3).

In referring to claim 2, 17, 27, 32 and 39,

- The trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, A certificate granting authority service, and A domain controller service:

  Fox Fig.1 shows the trusted third party includes a KDC.

In referring to claim 6, 8, and 21,

- Causing the trusted third-party to verify that the client has authorized delegation: Verifying authorized delegation is inherently implied in a system that uses Kerberos

In referring to claims 7 and 22,

- The trusted third-party includes a key distribution center (KDC):

  Fox Fig.1 shows the trusted third party includes a KDC

  Causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a restriction placed on the ticket originating from the client: Verifying authorized delegation is inherently implied in a system that uses Kerberos

In referring to claim 9, 23, and 34,

- The server is a front-end server with respect to a back-end server that is coupled to the front-end server:

  The proxy is a front-end server with respect to the client
- The back-end server is configured to provide the target service to which access is sought.

  The target service is a back -end server with respect to the client

In referring to claims 10 and 24,

- The trusted third-party includes a key distribution center (KDC):

  Fox Fig. 1 shows the trusted third party includes a KDC
- The KDC provides a ticket-granting-ticket associated with the client to the client; and the client does not provide the ticket granting ticket to the server:

  "During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy." (Fox, page 157, paragraphe 3)

In referring to claims 11 and 25,

- The trusted third-party includes a key distribution center (KDC):

  Fox Fig. 1 shows the trusted third party includes a KDC
- The server requests the new credential in a ticket granting service request message that includes a service ticket provided by the client to the server:

  "During the first step (illustrated in figure 1 b), the client uses the proxy as an intelligent router to obtain a TGT, which will then be managed by the proxy." (Fox, page 157, paragraphe 3)

In referring to claims 13, 14, and 15,

The implementation-specific identity information includes information selected from a group comprising privilege attribute certificate (PAC) information, security identifier information, Unix identifier information, Passport identifier information, certificate information: The system of Fox contains security identifier information

In referring to claims 40, 48, 49, 57, and 58,

- Identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

  "the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase" (Fox, page 157, paragraph 2)
- Causing a server that is operatively coupled to the target service and the client to request a

service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol:

- The server communicates with the client via the first authentication protocol which inherently implies identifying the client and the first authentication protocol
- Causing the server to request a new service credential, for use by the server and the target service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and the service credential to itself.

"Charon interaction consists of two distinct phases: the handshake phase, in which the client authenticates itself to the proxy via Kerberos and establishes a secure channel with it, and the service access phase, in which the proxy accesses Kerberized services on the client's behalf The Charon protocol module on the proxy and the Charon client-side software are responsible for the flow of control during both phases." (Fox, page 157, paragraphe 2)

causing the second authentication method trusted third-party to issue the new service ticith when one of : the service credential specifies that delegation of the service credential is authorized (Fox, Section 2.3, Page 158, Column 2, Paragraphs 1- 3); and the trusted third-party maintains an indication that the delegation of the service credential is authorized. (Fox, Section 2.3, Page 158, Column 2, Paragraphs 1- 3).

In referring to claims 41 and 50,

- The second authentication method trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service: Fox Fig.1 shows the trusted third party includes a KDC
-

In referring to claims 43, 52, and 60,

- The service credential is configured for use by the server and the target service to which access is sought.

"From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase." (Fox, page 157, paragraphe 3)

In referring to claims 44, 53, and 61,

- The credential authenticating the server includes a ticket granting ticket associated with the server.

  "From the point of view of the KDC and TGS, the proxy appears to be a normal Kerberos client during this phase." (Fox, page 157, paragraphe 3)

In referring to claims 45 and 54,

- Upon receiving a request for the new service credential from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation: Verifying authorized delegation is inherently implied in a system that uses Kerberos

In referring to claims 46 and 55,.

- The server is *a* front-end server with respect to a back-end server that is coupled to the front-end server; The proxy is a front-end server with respect to the client and the back-end server is configured to provide the target service. The target service is a back -end server with respect to the client

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which *forms* the basis *for all* obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 47 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox in view of Freier et al. *("The SSL Protocol Version 3.0",* 18 Nov 1996, hereinafter *"Freier").* Although Fox shows substantial features of the claimed invention, Fox does not show using SSL as the first authentication method. Nonetheless this feature is well known in the art and would have been an obvious modification to the system disclosed by Fox as evidenced by Freier.

In analogous art, Freier discloses SSL version 3.0. Freier shows SSL can be used to provide communication privacy over the Internet (abstract).

Given these teachings, a person of ordinary skill in the art would have readily recognized the desirability and advantages of modifying the system of Fox so as to use SSL, such as taught by Freier, in order to provide security for applications that don't support Kerberos authentication (For example, Outlook and Netscape email clients).

Conclusion

ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

The prior made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yasin Barqadle whose telephone number is 571-272-3947. The examiner can normally be reached on 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 571-272-3949. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained form the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either private PAIR or public PAIR system. Status information for unpublished applications is available through private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YB

Art Unit 2153